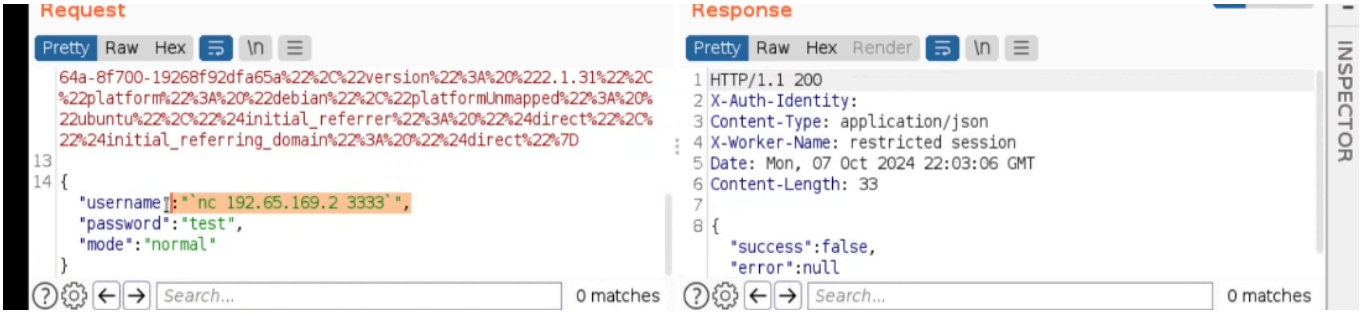
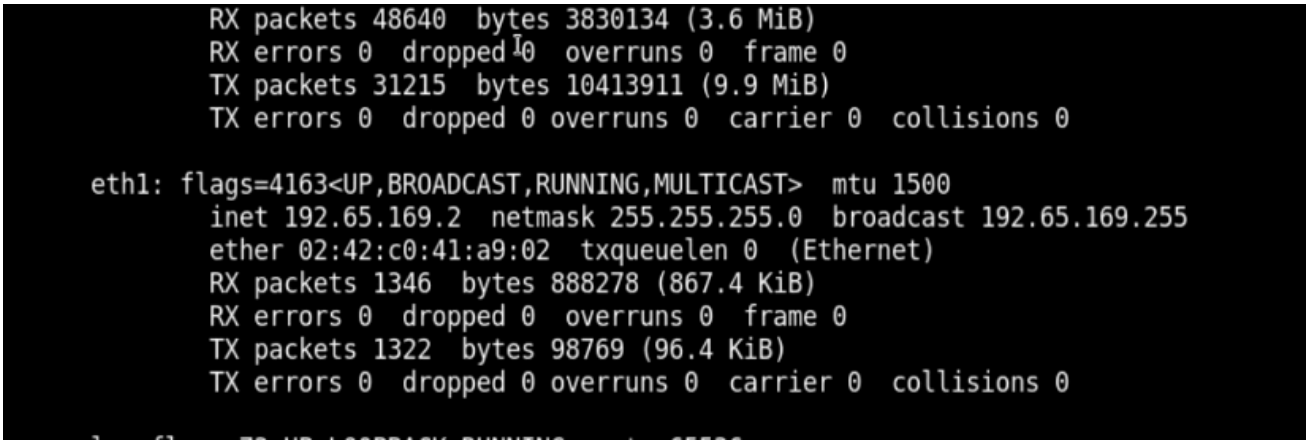
RCE

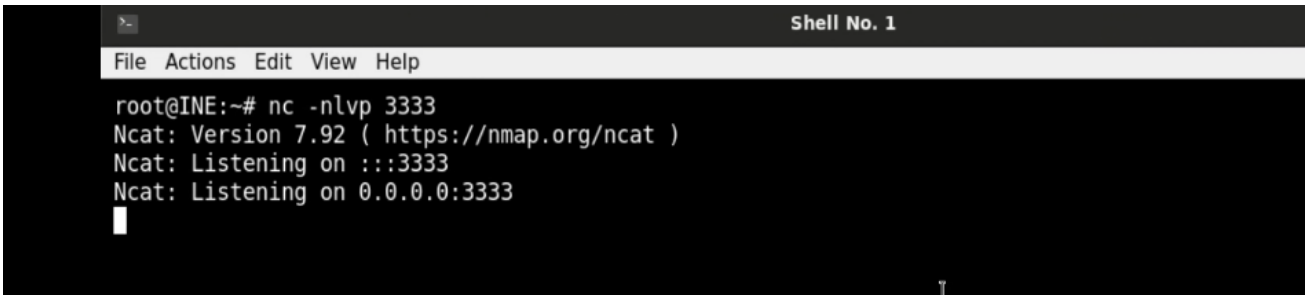
- الثغره دي عباره عن انك تقدر تنفذ كود او command عن بعد علي الويب ال نت بتحاول تخترقه
- تنصنيفها بيكون critical



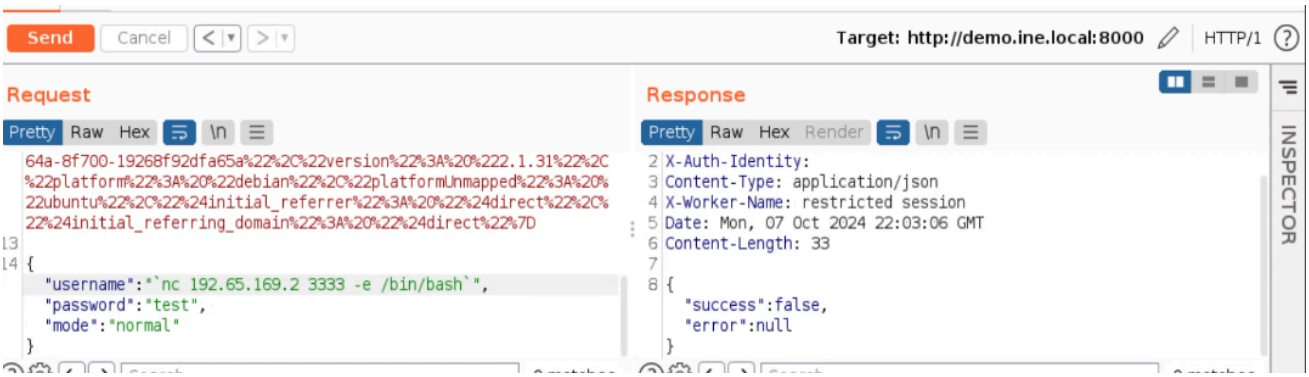
- هنا احنا لقينا json ف ممكن نجرب عليه عادي
- جربنا بالبرب اننا نوقف الطلب وننفذ اوامر
- بتحط الامر بتاعك بين ``
- ممكن تعمل ping علي رابط ال collaborator من البيرب برضو
- لو هوه مش json ممكن تجرب تعمل ملف ودا اشهر مسار
- /var/www/html/yousef.txt
- بتجرب اي امر لو اتنفذ تبقي الثغره موجوده



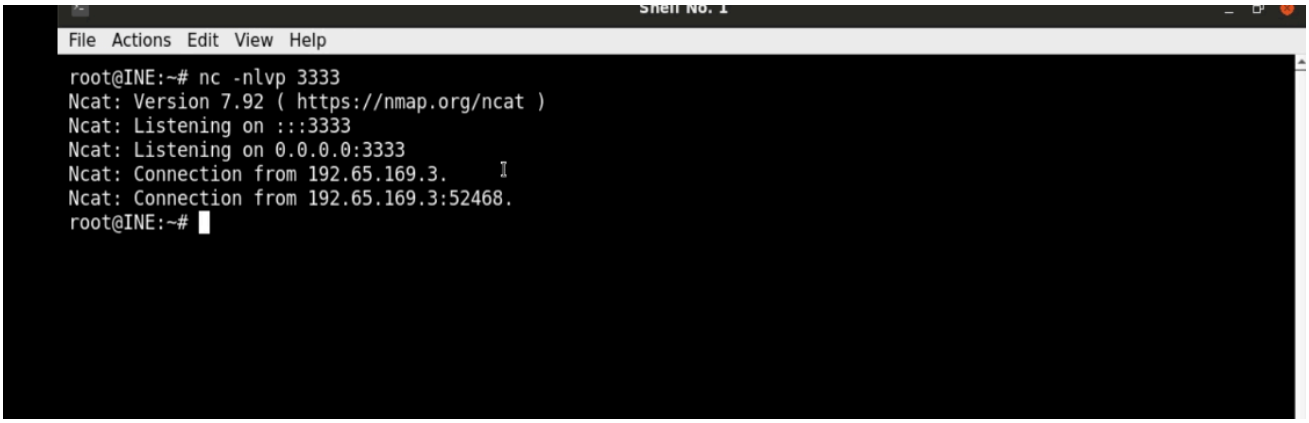
- جيب ال ip بتاع جهازك عشان تحاول تعلم ping عليه



- هنا شغلت port 3333 او اي منفذ غيره عشان تعمل اتصال بيه



- وحطينا الكود في request في حاله اتنفذ بيكون الموقع مصاب ل RCE
- هنا bin/bash عشان تعمل terminal هناك



- زي كدا اتنفذ وكدا شغال عمل Connection
